AMENDMENTS TO THE SPECIFICATION

Please amend the paragraph beginning on page 1, line 16 as follows:

In recent years, a content distribution service capable of distributing digital contents such as music, video and games ~~game~~ (hereinafter referred to as content) from a server apparatus to one or more terminal apparatuses through communication such as Internet, digital broadcast, Cable Television (CATV), and of using the content in one or more terminal apparatuses has been developed for a practical use. A common system used for the content distribution service uses a copyright protection technique for protecting a copyright of content in order to prevent an illegal use of the content by a malicious user. The copyright protection technique is, in ~~specific~~ detail, a technique of securely controlling use of content by a user such as reproducing the content or copying it to a recording media using an encoding technique, identifying technique and the like. Using the copyright protection technique allows a provider such as a content provider and a service provider to securely control the use of content in the one or more terminal apparatuses by a user.

Please amend the paragraph beginning on page 8, line 8 as follows:

The embodiment of the present invention will be specifically explained using the drawings as ~~following~~ follows.

Please amend the paragraph beginning on page 15, line 8 as follows:

The metadata 310, as shown in FIG. 5, includes the metadata body 311, the metadata signer ID312, and the digital signature ~~signer~~ 313.

Please amend the paragraph beginning on page 25, line 20 as follows:

Going back to the main routine of FIG. 9, in the case where the content provider ID212 and metadata signer ID312 correspond with each other, (i) the signature verification is executed (S102), (ii) the public key certificate 510 including the subject ID511 corresponding with the metadata signer ID312 of the digital signature of the metadata is obtained, (iii) the digital signature of the metadata is decrypted using the subject public key 512 included in the public key certificate 510, (iv) the hash ~~hush~~ values of the metadata body 311 and the metadata signer ID312 are compared, and verified whether or not they correspond with each other. In the case where the above mentioned hash ~~hush~~ values of the metadata body 311 and the metadata signer ID312 correspond with each other, as there has not been tamper, the metadata 310 is judged as possible to be used. On the other hand, in the case where the above mentioned hash ~~hush~~ values of the metadata body 311 and the metadata signer ID312 do not correspond with each other, as there has been tamper, the metadata 310 is judged as impossible to be used.

Please amend the paragraph beginning on page 26, line 17 as follows:

By such processes as described ~~describe~~ above, based on the signer identification information 4145 stored in the usage rules 414 of the license 410, it is possible to judge the use permission of the metadata signed by the content distribution server 20 or the metadata distribution server 30.

Please amend the paragraph beginning on page 27, line 20 as follows:

According to the present embodiment, the signer identification information 4145 is stored in the usage rules 414 of the license 410. However, the signer identification information 4145 may be stored in the ~~other~~ areas other than the usage rules 414 in the license 410. Also,

the signer identification information 4145 may be stored in the encryption content 210. Moreover, in the case where metadata is encrypted as well as the content, and there is a license of the metadata 310 including an encryption key, the signer identification information 4145 may be stored in the license of the metadata 310. In such cases as described above, the obtainment sources of the signer identification information 4145 respectively differ, but the same effects can be achieved in each case.

Please amend the paragraph beginning on page 29, line 19 as follows:

In the case where the one or more terminal apparatuses 60 do not have a secret key and a public key certificate, by encrypting the hash ~~hush~~ value of the metadata 310 using the domain key 112 or the intrinsic key, the same effects can be achieved.

Please amend the paragraph beginning on page 30, line 27 as follows:

In the control permission judgment of the metadata generated ~~generate~~ by the user (S201), the control permission information 4148 according to the metadata generated by the user is obtained from the usage rules 414 of the license 410. In the case where the control permission information 4148 according to the metadata generated by the user is "control possible according to the metadata generated by the user", the process is transited to the moving range judgment of the metadata generated by the user (S202).

Please amend the paragraph beginning on page 34, line 31 as follows:

Although only an exemplary embodiment ~~embodiments~~ of this invention has been described in detail above, those skilled in the art will readily appreciate that many modifications are possible in the exemplary embodiment without materially departing from the novel teachings

and advantages of this invention. Accordingly, all such modifications are intended to be included within the scope of this invention.